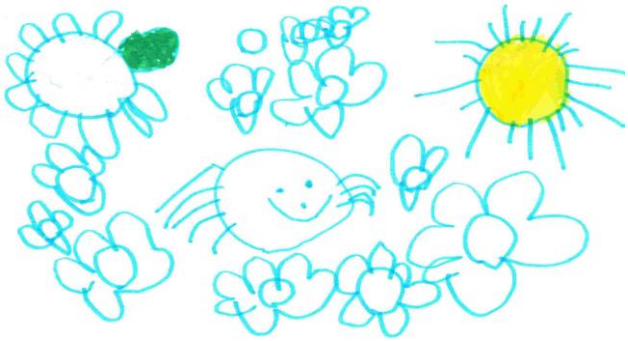


St. Thomas a Becket Nursery School
3 Tutts Barn Lane
Eastbourne
BN22 8XT

01323 725977

Registered Charity No. 1097448

Data:
- Collection
- Protection
- Retention
and
- In Transit

Responsibility: Trustees
Review Cycle: Every 3 years

Date of adoption / last review:	Signed / Role	Date of next review:
June 2024	CHarrison / Nursery Lead	June 2027

St Thomas a Becket Nursery
Data Protection and Security

EYFS January 2024

Information and record keeping

3.77 Providers must maintain records, obtain and share relevant information (with parents and carers, other professionals working with the child, the police, social services and Ofsted or their CMA, as appropriate). This is to ensure their setting is safe and efficiently managed, and the needs of all children are met[45]. Providersmust enable a regular two-way flow of information with parents and/or carers (and between other providers, if a child is attending more than one setting). If requested, providers should incorporate parents' and/or carers' comments into children'srecords.

3.78 Records must be easily accessible and available (these may be kept securely off the premises). Confidential information and records about staff and children must be held securely and only accessible and available to those who have a right or professional need to see them[46]. Providers must be aware of their responsibilities under the Data Protection Legislation[47] and, where relevant, the Freedom of Information Act 2000.

3.79 Providers must ensure that all staff understand the need to protect the privacy of the children in their care, as well the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality. Parents and/or carers must be given access to all records about their child, provided that no relevant exemptions apply to their disclosure under the Data Protection Act [48].

3.80 Records relating to individual children must be retained for a reasonable period of time after they have left the provision[49].

45 Guidance on sharing information with relevant services when there are safeguarding concerns is available via: Information sharing advice for safeguarding practitioners - GOV.UK (www.gov.uk)

46 The National Cyber Security Centre (NCSC) has published helpful guidance on cyber security: https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings

47 This includes the Data Protection Act 2018 and General Data Protection Regulation 2018 see: Data protection: The Data Protection Act - GOV.UK (www.gov.uk)

48 The Data Protection Act 2018 (DPA) gives parents and carers the right to access information about their child that a provider holds. However, the DPA also sets out specific exemptions under which certain personal information may, under specific circumstances, be withheld from release. For example, a relevant professional will need to give careful consideration as to whether the disclosure of certain information about a child could cause harm either to the child or any other individual. It is therefore essential that all providers/staff in early years settings have an understanding of how data protection laws operate. Further guidance can be found on the website of the Information Commissioner's Office at: https://ico.org.uk/fororganisations/guide-to-the-general-data-protection-regulation-gdpr/

49 Individual providers should determine how long to retain records relating to individual children.

Information about the child

3.81 Providers must record the following information for each child in their care:

• Full name

• Date of birth.

• Name and address of every parent and/or carer who is known to the provider.

• Information about any other person who has parental responsibility for the child.

• Which parent(s) and/or carer(s) the child normally lives with.

• Emergency contact details for parents and/or carers.

Statement

We hold personal data about our employees, children and their families and other individuals for a variety of nursery purposes. This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Nursery Lead be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, statutory and legislative purposes, payroll, consultations and business development purposes. Nursery purposes include the following: - Compliance with Ofsted and other legal and regulatory obligations and good practice - Gathering information as part of investigations for safeguarding purposes or in connection with legal proceedings or requests - Ensuring nursery policies are adhered to (such as policies covering email and internet use) - Operational reasons, such as training and quality control, ensuring the confidentiality of sensitive information, security checking - Investigating complaints - Checking references, ensuring safe recruitment and working practices, monitoring and managing staff absences, administration and supervisions - Monitoring staff conduct, disciplinary matters - Promoting nursery services - Improving services
Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, volunteers and students, contract and bank staff, suppliers and marketing contacts, members of the public.

	Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, contact details, correspondence, emails.
Sensitive personal data	Personal data about an individual's physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data will be strictly controlled in accordance with this policy.

This policy applies to all trustees and staff. All must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to acceptable use, internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Procedures

Fair and Lawful Processing

Personal data must be processed fairly and lawfully in accordance with individuals' rights. This generally means that we will not process personal data unless the individual whose details we are processing has consented to this happening.

The Nursery Lead will:

- Keeping the staff and trustees updated about data protection responsibilities, risks and issues
- Review all data protection procedures and policies on a regular basis
- Assist with data protection training and advice for all staff members and those included in this policy
- Answer questions on data protection from staff and trustees
- Respond to individuals such as parents and carers who wish to know which data is being held on them by St Thomas a Becket Nursery
- Ensure all equipment meet acceptable security standards

The processing of all data must be:

- Necessary to nursery practice
- In our legitimate interests and not unduly prejudice the individual's privacy

Our Privacy Notice

- Sets out the purposes for which we hold personal data on employees and service users
- Provides that service users and correspondents have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure safeguarding). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Nursery Lead.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Nursery Manager so that they can update your records.

Data security

Personal data must be kept secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Nursery Lead will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely – in situ or in Transit

- In cases when data is stored on printed paper, it is kept in a secure place where unauthorised personnel cannot access it
- Printed data is shredded when it is no longer needed
- Data stored on a computer is protected by strong passwords.
- Cloud based storage is based in England and is secure.
- All data is protected by security software and strong firewall.

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Subject Access Requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

Any subject access requests should be referred immediately to the Nursery Lead.

Please contact the Nursery Lead if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

Any request from an individual not to use their personal data for direct marketing purposes will be honoured.

We do not send direct marketing material to anyone electronically (e.g. via email).

Data Protection Act Provisions (and GDPR)

Our Privacy Notice and Subject User Access are clearly displayed on our website for full transparency of data protection purposes.

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our nursery. Our records and retention information offers details on how we collect data and what we will do with it. Please ask if you wish to see a copy.

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Data audit and register

Data audits manage and mitigate risks that inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

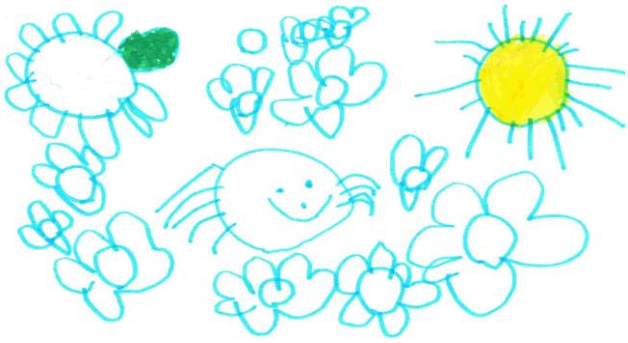
All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both the individual and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.



St. Thomas a Becket Nursery School
3 Tutts Barn Lane
Eastbourne
BN22 8XT

01323 725977

Registered Charity No. 1097448

Data Retention Schedules

Retention Schedule
The EYFS Framework January 2024
3.80 Records relating to individual children must be retained for a reasonable period of time after they have left the provision
49. 'Individual providers should determine how long to retain records relating to individual children.'

At St Thomas a Becket Nursery we will retain children's records for a period of 5 years following their leaving date from nursery.

Field Description:

Class Code
A unique reference for ease of reference and for transferring records

Class Name
How groups of records are known

Retention Notes
The reason for the action. Retention periods are based on legal and business need

Retention Period
The length of time the record is kept for

Disposal Trigger
What triggers the retention period (e.g. end of financial year)

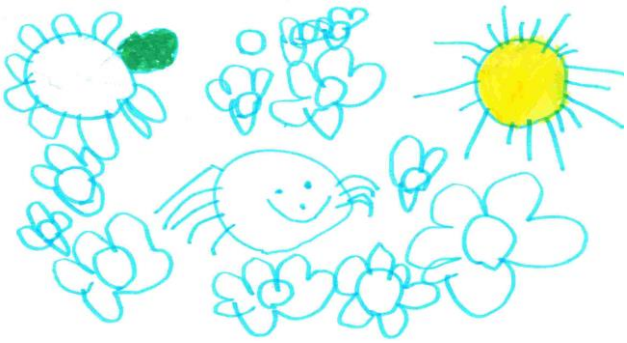
Action -What happens at the end of the retention period.
Records are:
Destroyed
reviewed for extended retention

PD
Whether the record contains personal data ('Yes', 'No', 'P' for 'potentially')

Class Code	Class Name	Retention Notes	Retention Period	Disposal Trigger	Action	PD
A1	Inspection reports resulting from inspections carried out by Ofsted	Nursery Improvement and reference needs, kept by Ofsted.	Until next inspection	Superseded	Destruction	No
B1	Complaints	Nursery Improvement and reference needs. Serious complaints kept by Ofsted.	3 years.	Term 6 following third year from date of complaint	Destruction	No
C0	Nursery Place Waiting List	Business Need	2 years	Term 6	Destruction	Y
C1	Children's Records – including: name, home address and date of birth name, home address and telephone number of their parent/guardian/carer	Ofsted Registration Requirements - Child Information sheet	7-21 years following child nursery leaving date	Term 6	Destruction	Y
C2	Daily record of their name and hours of attendance	Ofsted Registration Requirements - Registers	7-21 years following child nursery leaving date	Term 6	Destruction	Y
C3	Medicine given, including the date, circumstances and who gave it (this includes medicine that the child takes themselves) and a record of their parent/guardian/carer's consent	Ofsted Registration Requirements - Child medicine sheet	21 years of age	Term 6 of birth year	Destruction	Y
C4	Nappy changing / toileting / sleep records	Nursery records	21 years of age	Term 6 of birth year	Destruction	Y
C5	Accidents / Incidents on the premises	Ofsted Standards - Accident Records	21 years of age	Term 6 of birth year	Destruction	Y
C6	SEND records	Support services for individual child	Records are Confidentially transferred to the Transition setting / school	(or until child reaches age of 24)	Destruction	Y
C7	Safeguarding	Recording of low level concerns and any Early Years Help records	Records are Confidentially transferred to the Transition setting / school	(or until child reaches age of 24)	Destruction	Y
C8	Child Protection records	Held by ESCC. See their Document Retention Schedule – class code CF21	Records are Confidentially transferred to the Transition setting / school	(or until child reaches age of 24)	Destruction	Y

C9	Looked After Children – all records except those being passed on confidentially to transition setting / school	Safeguarding	21 years following child nursery leaving date	Term 6 following	Destruction	Y
D1	Name, home address and telephone number of everyone living or working where you provide childcare	Ofsted Standards - Staff records	N/A	N/A		Y
D2	Personal records, performance appraisals, employment contracts, pay, employment benefits/ PAYE etc	Legal and business. (potential tribunals for the 3-month risk period during which terminated employees can bring a claim against you, but it could be used for defending a county court or high court claim, which can occur many years down the line)	6 years	Term 6 or 1	Destruction	Y
D3	Recruitment records including non-successful candiates	Legal and business. (The period of time during which a discrimination claim could be brought against your organisation.)	6 months	Term 1 or Term 4	Destruction	Y
D4	DBS checks - Date of issue, name of adult, type of disclosure, position / role; URN.	Safeguarding and Ofsted	Whist employed / volunteering etc. Then as per ex staff records			
D5	Visitors Records	Legal and Business Safeguarding	25 years		Destruction	P
H1	Fire Drill Records	Legal and Business	5 years	Term 1 following	Destruction	N
H2	Risk Assessments	Legal and Business	5 years	Term 1 following	Destruction	
H3	Building and Maintenance Records	Legal and Business	5 years	Term 1 following	Destruction	N
H4	Serious incidents or accidents	Legal; Health and Safety	As per RIDDOR guidance		Destruction	
T1	Trustee Meeting Minutes	Legal and business.	During existence of the Nursery		Archive	P
T2	Accounts, Insurance	Legal and business.	During existence of the Nursery		Archive	
T3	Ex – Trustee information	Legal and business	6 years	Term 1	Destruction	Y

	Type of Record	Retention Period
	Adult – Allegation	Normal retirement age or for 10 years – whichever is longer (IRMS, 2019; Department for Education, 2021).
	Adult – Allegation Unfounded / Malicious	As above regardless of whether the allegations were unfounded. However, if allegations are malicious, destroy immediately.
		Records relating to concerns about an adult's behaviour should be kept in the person's confidential personnel file (not in a central 'concerns log') and a copy should be given to the individual.
	Child Protection / Safeguarding	Storage of child protection records: Child protection records are electronic or paper-based and are kept confidential and stored securely. Electronic files are stored on computers supported with encryption for protection against hackers and viruses. • Information about child protection concerns and referrals are kept in a separate child protection file for each child. The child protection file is started as soon as we become aware of any concerns. • Child protection files are kept separately from a child's general records. You should mark the general record to indicate that there is a separate child protection file. • All record sharing is on a need to know basis and shared in a confidential manner by using passwords and encryption for sharing/receiving electronic files. • Staff and volunteers do not use personal computers to make and store records. • Both DSLs are responsible for managing our child protection records. Should both leave our nursery, we will appoint somebody to take over their role and arrange a proper handover.
		Child protection files should be passed on to any new school a child attends (Information and Records Management Society (IRMS), 2019; Department of Education, 2016; Department for Education (DfE), 2021).
		Until the child is 25 (this is seven years after they reach the school leaving age) (Information and Records Management Society (IRMS), 2019).
		In some cases, records should be kept for longer periods – see the 'Exceptions' section below for more information.
	Staff – ex	6 years



St. Thomas a Becket Nurser
3 Tutts Barn Lane
Eastbourne
BN22 8XT

01323 725977

Registered Charity No. 1097448

Data in Transit

Statement
St Thomas a Becket Nursery practices safety of electronic communications and record keeping in line with the General Data Protection Regulations whilst awaiting any government review of rules and regulations inherited from the EU post Brexit.

The aims of the policy are to ensure that the use of removable storage devices is accomplished with due regard to:

- Maintaining the safety and integrity of the data
- Maintaining high standards of care towards data and information about nursery children, staff or information that is exempt from disclosure
- Compliance with legislation, policies or good practice requirements

Nursery use secure cloud-based storage and discourage the use of removable media for data transfer, except for the regular use on the premises of the practitioner used tablets. The nursery accept that there may be times that data may be needed to be moved or accessed to other sources in the best interests of the child's wellbeing, such as liaising with external agencies and transferring of records such as safeguarding and medical records.

This policy addresses the committed security measures of St Thomas a Becket Nursery. Additional best practice guidance will also be sought from the below if thought necessary and tailored to fit our nursery administration.

DfE Data Protection Toolkit for Schools: For information on what schools need to do in order to comply with data protection regulations

1.1 This policy supports the controlled storage and transfer of information by Staff and Trustees of St Thomas a Becket Nursery who have access to and use of computing equipment that is owned by St Thomas a Becket Nursery.

1.2 Information is used in the nursery and is sometimes shared with external organisations, such as East Sussex County Council Children's Services / ISEND / Other health professionals. In this instance, confidential information is sent and received securely via encrypted email.

1.3 It is essential for the continued operation of the nursery that the availability, safety, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to the nursery's needs. All of our electronic devices that are used for storing images or children's data, are encrypted and password protected.

2 Scope

2.1 This policy sets out the principles that will be adopted by the nursery in order for material to be safely stored so that the risk of loss or corruption to data is low.

2.2 The use of removable media for nursery purposes must be limited to the following, excepting bullet point 2.3 below: the Nursery Laptops and the 5 x St Thomas a Becket practitioner 'tablets'. Nursery reject the use of all other removable media for personal data due to their small size and thus high risk of removable media being mislaid or damaged.

2.3 It is acknowledged that the Nursery Lead and Nursery Manager may need remote access to the Nursery email account and that this may be accessed by password protected and or encrypted (individual / not shared) mobile phones. Any email account log in will additionally be security protected via our email security setting, in which any log in attempt from an unfamiliar device will be flagged and an authorisation request be necessary.

2.3 The Policy does not apply to the use of ICT equipment used in nursery for curriculum purposes but does apply to ICT used for nursery administration purposes.

2.4 Any person who intends to store nursery data on removable media must abide by this Policy and must do so with the authority of the trustees or Nursery Lead. The individual may be held personally liable for any breach of the requirements of this policy.

2.5 Failure to comply with this policy could result in disciplinary action.

3 Responsibilities

3.1 Management are responsible for enforcing this policy and for having arrangements in place to identify the location of all removable media used in connection with Nursery business.

3.2 Users of removable media must have adequate Records Management / Information Security training so that relevant policies are implemented.

3.3 All devices used in transit of data must be properly protected with encryption and user passwords.

4 Incident Management

4.1 It is the duty of all employees to not allow storage media to be compromised in any way whist in their care or under their control. There must be immediate reporting to the Nursery Lead or the Trustees of any misuse or irresponsible actions that affect work

data or information, any loss of material, or actual, or suspected breaches in information security.

4.2 It is the duty of all staff to report any actual or suspected breaches in information security to the Nursery Lead or the Trustees.

5 Data Administration

5.1 Where there is a business requirement to distribute information to third parties, then the file must sent by secure electronic means.

6 Security

6.1 All storage media must be kept in an appropriately secure and safe environment that avoids physical risk, loss or electrical corruption.

6.2 Virus and malware checking software approved by 'UNISERVE' must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded.

7. Use of removable media

7.1 Care must be taken over what data or information is transferred onto removable media such as the tablets. Only the data that is authorised and necessary to be transferred should be saved on to the devices rather than held in a secure cloud.

7.2 Safeguarding data must not be stored on the tablets at any time.

7.3 Nursery material belongs to the Nursery and any equipment on which it is held should be under the control of the Nursery and not available to be used for other purposes that may compromise the data.

7.4 The person arranging the transfer of data must be authorised to make use of, or process that particular data. Whilst in transit or storage the data must be given appropriate security according to the type of data and its sensitivity.

7.5 Encryption and password protection must be applied to the nursery storage media. If encryption is not available (NurseryLead and Manager mobile phones for email access) then password / passcode control must be applied both on the device and to access the email account.

7.6 Removable data may be used by staff / students to transit nursery documents that do not contain any personal data, such as nursery policies etc

8 Breach procedures

8.1 Users who do not adhere to this policy will be dealt with through the nursery's disciplinary process.